User Manual

Version 3.1.5.0

Contents

User Manual 1

Why read this manual? 5

What is CyberSentinel? 6

CyberSentinel Key Features 7

Why use Categories? 10

Computer Requirements for CyberSentinel 12

Installation Process 13

How to login to the CyberSentinel Console 15

Removal of CyberSentinel Software 16

Exploring CyberSentinel 17

Configuring a user account for testing 18

Running the word capture test 21

How to run the website test 22

How to tell what machines are monitored by CyberSentinel 23

How to Add a User to CyberSentinel 25

How to delete a user from CyberSentinel 26

How to copying settings from one user to another 27

Recommended User Settings..... 29

Configuring a user's Monitored Words..... 31

What is in the word libraries? 33

The 'My Word' Libraries..... 34

How often should the word monitor work?..... 37

Different CyberSentinel modes..... 38

How to log Websites 39

How to Log Internet Chat..... 40

Offline Settings 41

Configuring a User's Web Safety..... 42

Website filtering by library categories 45

Website and word scanning differences 46

Using Website Category Scanning 47

Time Management 50

Setting up an Acceptable Use Policy 53

The Family Summary Data..... 54

The User Summary Data..... 56

Viewing Capture Data **58**

Viewing Chat Data **59**

Viewing Web Log Data **60**

Reports **61**

What are my account details? **63**

How do I change my email address? **64**

How do I change my password? **65**

Audit Messages **66**

What is an Acceptable Use Policy? **67**

Can I receive emails from CyberSentinel? **68**

How long is my license is valid for? **69**

Glossary **70**

Further Help and Support **72**

Index **73**

Why read this manual?

If you are a Parent/Carer responsible for children who use computers and you are also

- ✓ Concerned that those children are not upset by reading unsavoury text
- ✓ Amazed at the language that is used in chat sessions
- ✓ Worried that the children will think that you are invading their privacy
- ✓ Reluctant to keep nagging about spending too much time on the computer
- ✓ Want to set different permissions for different aged children
- ✓ Sensitive to the need for privacy and freedom of expression

We want you to ensure that the CyberSentinel Software is properly set up for your family.

Note concerning screen captures

Screen captures may contain offensive material. In this manual we have 'blanked out' the nasty bit so as not to shock or offend you.

Please be aware that the screen captures that are generated and viewed when the program is in actual use will not 'blank out' the cause of the violation or other inappropriate material on the screen.

Please ensure these images are viewed with extreme caution and never publicly exhibited or shown to anyone who is unprepared for such images.

What is CyberSentinel?

CyberSentinel is an e-Safety software product designed to automatically integrate into your Internet-enabled home computer with minimal impact on the general use of it

All the data collected by CyberSentinel is stored on our secure server, and you view and update it using a secure website.

CyberSentinel consists of

- ***Monitoring software*** that you install on your computer.
- ***Database*** for storing data logs and user profiles
- ***Website*** for displaying data logs and updating settings that is managed by us

The database and website components are located on computers accessible across the Internet and managed by us. Only the software itself is present on your computer(s).

What it does

CyberSentinel will monitor and report about the computer activities that you choose for each user account on all computers running this software, all the time.

How it works

CyberSentinel applies configuration rules that you set and takes visual records – in screen captures – known as 'captures' of possible violations and logs data on computer usage. The captures and logs are immediately sent over the internet and stored in your secure section of our database on our servers.

When you login to the CyberSentinel website on the internet, your data is retrieved from the database and displayed.

From time to time, you should revisit your rules as your users get older and you trust them to experience the internet unescorted.

CyberSentinel Key Features

Regularly checks for inappropriate words/phrases

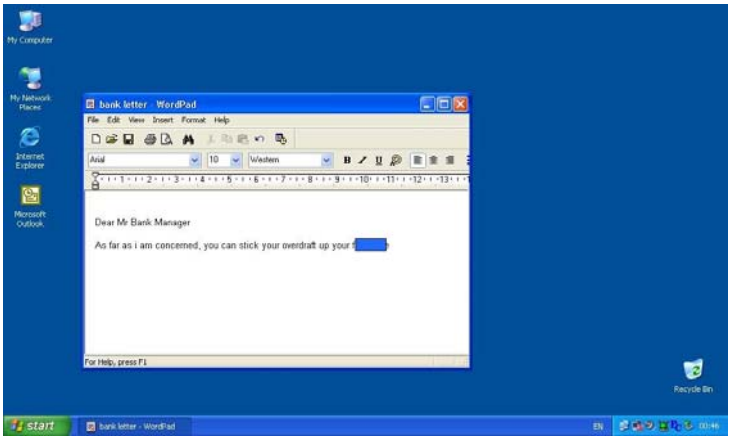
Every minute or so, CyberSentinel checks all the words displayed on the desktop – this can not include words that are part of pictures. The characters found are compared to words and phrases contained within a set of built-in word/phrase libraries. You can choose which libraries are to be included in the search.

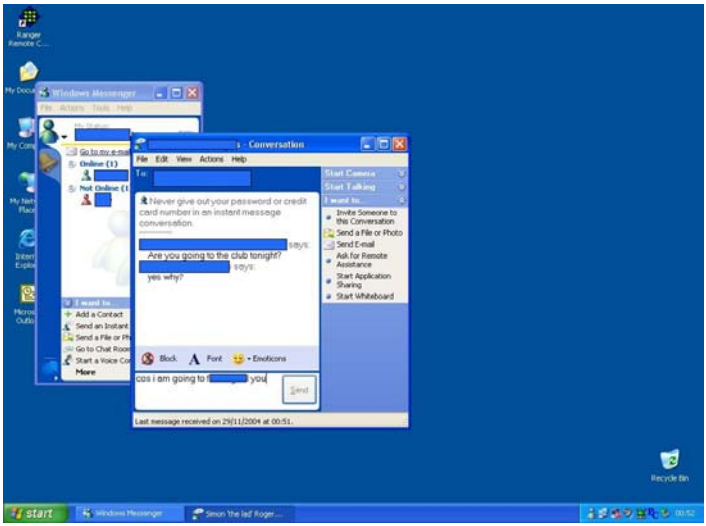
If a match is found, a full screen capture will be taken straight away just as if you were to press the 'Print Screen' button at the computer.

The following data is stored along with the screen capture

- User logged on
- Computer name
- Date and Time
- Word that generated the screen capture
- Application (or 'URL') where word was found

Here are two example screen captures:





The screen capture will be sent over the internet to the CyberSentinel server and stored in your secure part of the database.

You should log on to the CyberSentinel Console regularly to check if there have been any captures taken. You can then decide if it's necessary to discuss this with your user and the appropriate action to take.

Monitors web sites

Every time a user tries to open a webpage, the URL is compared to lists of websites that are known to be inappropriate. These lists are grouped into categories to allow you to determine which categories are not suitable for each of your users.

The URL lists are updated regularly by us at CyberSentinel.

If you like, you can easily create a 'white list' of your own for your user to ensure that they are only visiting websites that you know to be safe and suitable when you are not there with them.

For older children, you can create a special 'black list' stopping them from accessing sites that might be preventing them from getting on with their homework!

If you want, CyberSentinel can record statistics about all web sites that a user visits, these include average duration of the visit and how many times that site has been visited and the time of the last visit. This allows you to see a profile of your child's use of the internet.

Supervises Time

You can configure access to the internet for different users on a timed basis. This will help you ensure that older children will not be able to use the internet in the middle of the night without you having to be there to check.

If you like, you can specify how many hours a user can be on the computer per day. This takes away the need for you to try and negotiate this on a daily basis and allows you to provide older child with a computer time quota for entertainment as well as homework. If you have fewer computers than users, or want your children to do other things, this invaluable tool will help stop arguments!

Logs Chat

If you want, CyberSentinel can record and store entire transcripts of chat conversations. You can review the conversations and ensure that your child is behaving safely online. Note, not all chat programs are supported. See our website for full details of the currently supported chat clients.

Gets Agreement

If you want to ask your children to agree to the rules of using the computer without having to nag, CyberSentinel can display your family's Acceptable Use Policy (AUP) at each logon.

Each user must click on the 'accept' button to acknowledge the rules before they can use the computer.

Why use Categories?

CyberSentinel monitors both words and websites via category groups rather than individually, allowing you to be able to monitor computer use simply.

The main strength of CyberSentinel is in monitoring words and phrases. We believe that this is the most powerful means of protecting your children on the internet as it does not rely on having to keep a list of websites up to date, the websites may change, but the words that are used in them remain largely the same.

We group the words and phrases into the following categories to allow you to monitor them in groups: Pornography, Strangers, Profanity, Acronyms, Drugs, Self harm, Racism and Hate/violence. When one (or more) of the words is detected by CyberSentinel, a screen capture is taken and the user can go on working – if they are in visible mode they will get a warning on the screen that the capture was taken.

Websites are also grouped into categories, although they are slightly different to reflect types of websites rather than contents of the websites. There are undesirable categories probably unsuitable for children like drugs and alcohol, pornography, gambling and shopping. Then there are fun categories including games, entertainment, music, social networking, and webmail. At different times you might block each. If the user tries to access a website in a blocked category, s/he will be re-directed to a blank page instead.

Remember that if you are monitoring words in the Profanity category (or any other category), these will cause a screen capture to be taken when encountered in a website, whether it is blocked or not.

Prepare for a CyberSentinel Installation

This is what you should do before installing CyberSentinel on your home computers.

- ✓ Check that your home PC(s) is suitable for installation
- ✓ Discuss what you intend to do with your children and create an Acceptable Use Policy with your family

- ✓ Think about the types of restrictions and monitoring you want to impose on your children. Don't restrict things too much to start or you'll put them off using the computer at home.

When all these tasks are done, download and install CyberSentinel on your computers. Follow the installation and setup instructions carefully to configure a few settings to get you going.

Computer Requirements for CyberSentinel

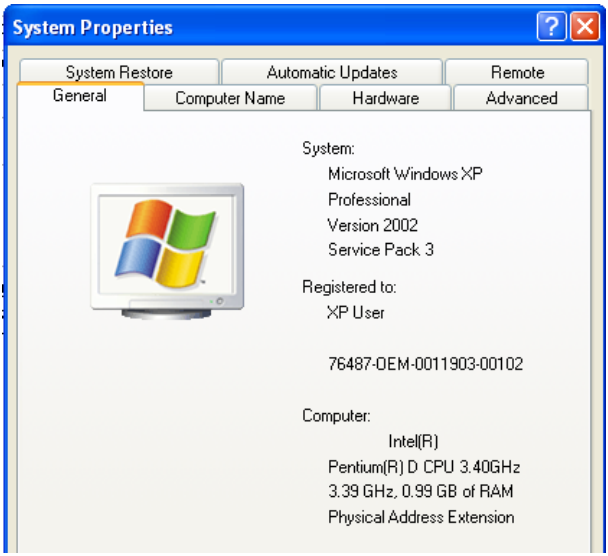
Hardware Requirements

CPU	1Ghz or faster Pentium® compatible
Memory	128MB RAM (256MB recommended)
Storage	100MB free space

Software Requirements

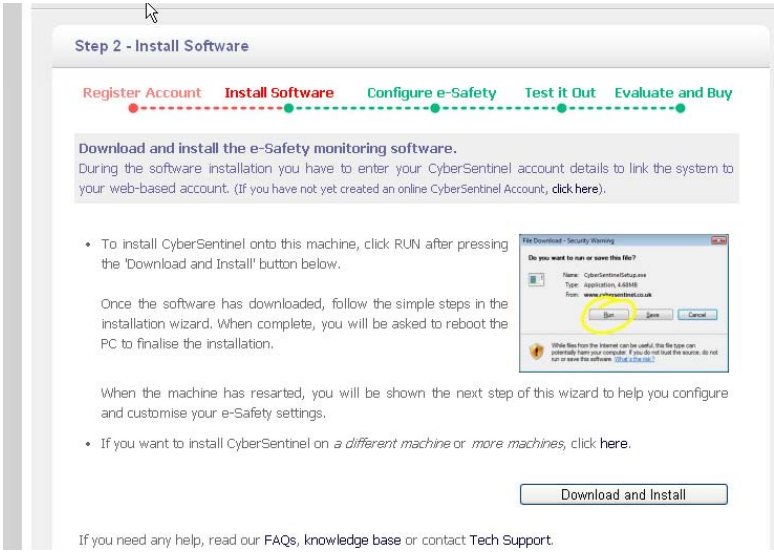
Operating System	Windows XP Professional
	Windows XP Home Edition
	Windows Vista

You can tell if your computer complies with this by displaying the System Properties window from the control panel. Only computers purchased before 2000 would be unsuitable!



Installation Process

The installation process is fully documented in the e-Shop on our website, including screen shots of each stage and opportunities to get technical support if required.


Step 2 - Install Software
Register Account
Install Software
Configure e-Safety
Test it Out
Evaluate and Buy
Download and install the e-Safety monitoring software.
During the software installation you have to enter your CyberSentinel account details to link the system to your web-based account. (If you have not yet created an online CyberSentinel Account, click here).
To install CyberSentinel onto this machine, click RUN after pressing the 'Download and Install' button below.
Once the software has downloaded, follow the simple steps in the installation wizard. When complete, you will be asked to reboot the PC to finalise the installation.
When the machine has resarted, you will be shown the next step of this wizard to help you configure and customise your e-Safety settings.
If you want to install CyberSentinel on a different machine or more machines, click here.
Download and Install
If you need any help, read our FAQs, knowledge base or contact Tech Support.

The following is a brief description of the process.

Registration

Register your account at the e-Shop to create your secure data storage area.

The information that we store about you is minimal, designed to protect your data.

Installation

Any computer that you own and that has access to the internet can have the CyberSentinel home software installed on it. Download and run the software from the e-Shop straight to the computer (you will need to be the administrator to do this) and it will work straight away.

Complete re-installation of the client software is rarely (probably never) required as we automatically update the software when updates become available.

Customisation

Once the software has been installed on your computers, data will start being sent to your web-based database as soon as users start using them. You don't need to do anything else for a basic installation.

You can log on to the web-based console at any time (via our website) to change the user's e-Safety settings to reflect their age and your level of trust.

Evaluate and Buy

You have 30 days to evaluate and test the software before purchase.

Installation Process

It is important that the program is installed on all computers that your children are likely to use.

Follow the following steps at each computer that will be monitored:

Step 1. Logon to the computer to be monitored as an administrator (or a user with equivalent permissions)

Step 2. in a web browser, navigate to the e-Shop website www.cybersentinel.co.uk

select the 'Shop' page

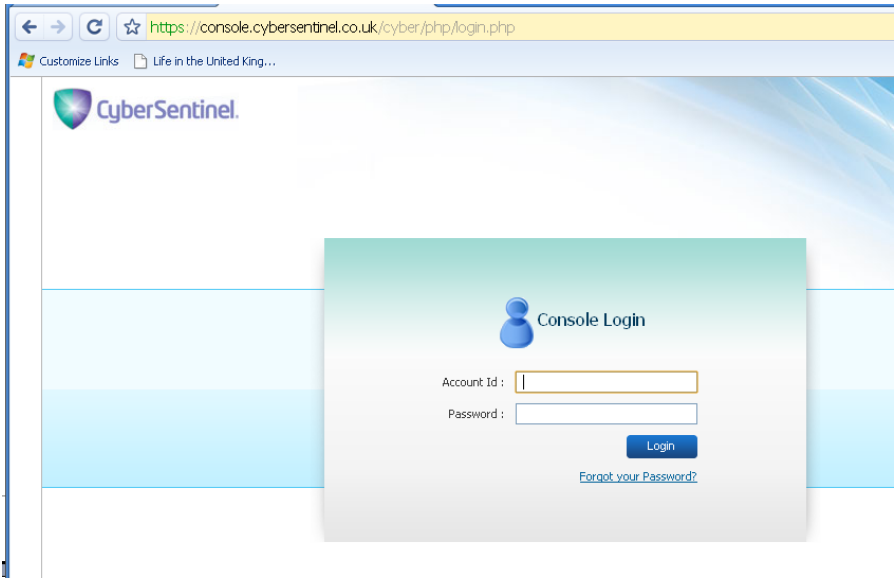
Step 3. follow the detailed instructions there for registering, downloading and installation.

The CyberSentinel home software is now active.

How to login to the CyberSentinel Console

To view the logs of data and any captures that have been taken, as well as to customise the user settings, you use the web-based console. As this is a website, you can access it from any internet connected computer in the world.

Step 1. Open a web browser and navigate to https://console.cybersentinel.co.uk



Type your account Id and password that you used to register your account into the boxes.

Note that if you have forgotten your password, you can click on the 'forgot password' link to reset.

Press the Login button to go to your Home screen containing a summary of the recent computer activity occurring on your computers.

Removal of CyberSentinel Software

CyberSentinel software can be removed from the home computer at any time. The administrative logon for CyberSentinel must be used to allow removal of the software.

You will have to remove the software from all computers individually.

Step 1. **Open the Control panel**

Step 2. **Open Add/Remove programs.**

Step 3. **Locate cybersentinel.exe in the list and click on it**

Select the remove option and the password dialog will be displayed.

Step 4. **Enter your Account Id and password for CyberSentinel that you would use to access the console.**

Client software removal will begin immediately if the correct details are entered. The completion dialog is displayed when this has finished.

Step 5. **Select 'Finish' to exit the program**

The client software has now been removed from this computer.

Repeat this procedure on other computers where you have installed the home software.

Exploring CyberSentinel

To explore the full potential of CyberSentinel it is easiest to configure some dummy data. You will need to test users individually so will require the user logon for each user that you plan to test.

You could do this with each child to show them the process so that they will really understand how it works.

You need to know:

- The logon name for each user that you are testing and the password
- The machine that they will be using
- The web address of the console
- Your logon details for the console

You will be testing that

- Bad words will cause a violation to trigger a screen capture
- Websites will be logged

The steps to take are:

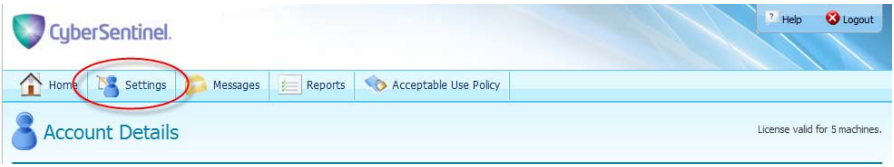
- ✓ Login as an administrator on your computer
- ✓ Install the CyberSentinel Home software on the computer
- ✓ Open your CyberSentinel console
- ✓ Confirm that the machine is registered correctly
- ✓ Configure the console for testing
- ✓ Test by using the computer
- ✓ Refresh the console
- ✓ Check the results on the console

Configuring a user account for testing

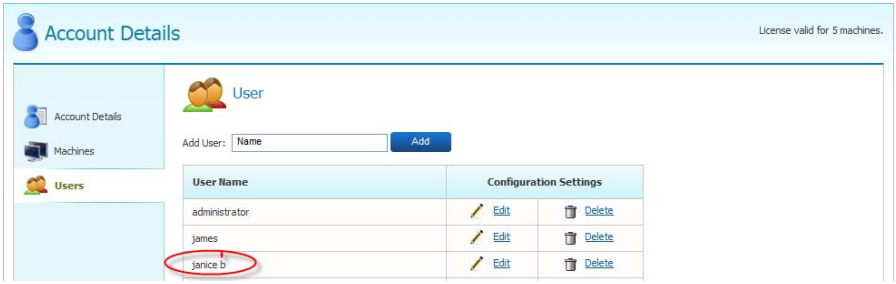
You need to configure each user separately.

For testing, you should set the maximum warnings on for the computer so that you can be sure that CyberSentinel is working correctly.

Step 1. Choose the 'Settings' tab



Step 2. Choose the User tab



Step 3. Select the user you would like to test

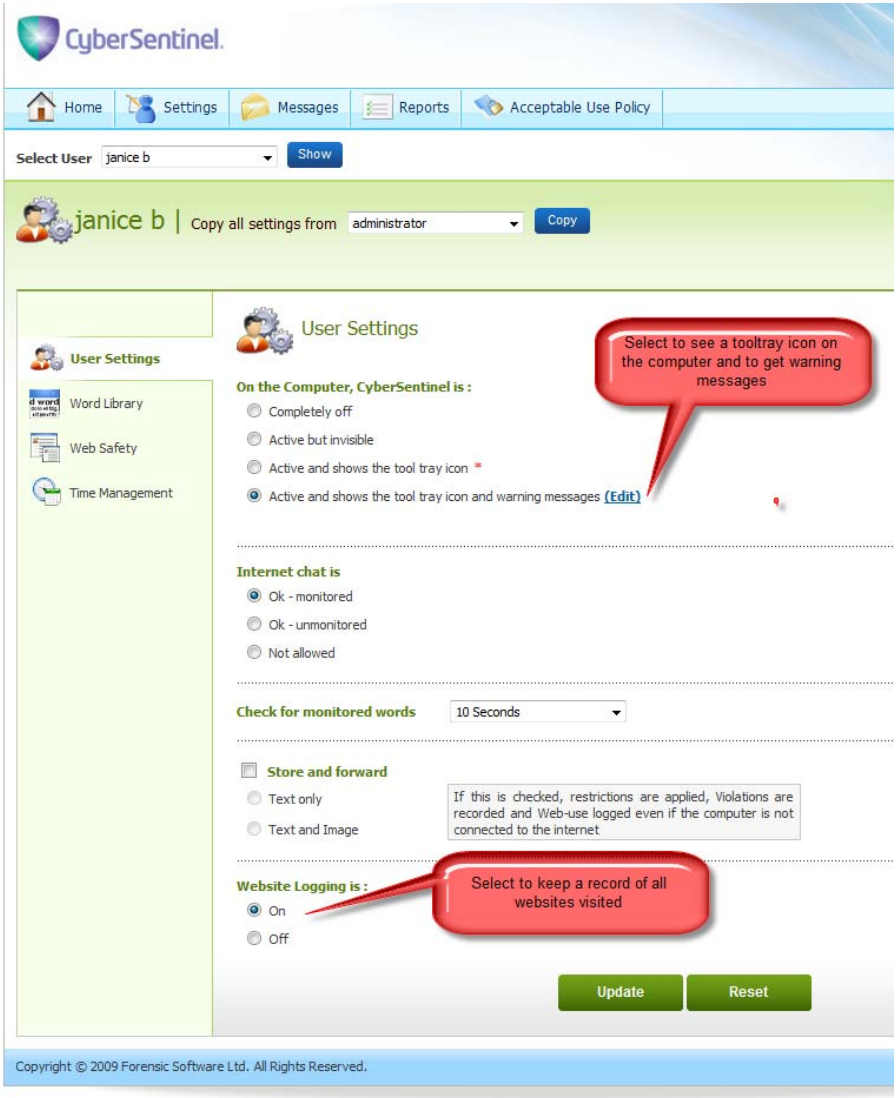
The users shown will be the names of any users that have used the machine since CyberSentinel was installed. If the user is not shown in the list, then simply log in as that user (on the PC you have installed CyberSentinel). After a few minutes refresh this page and the console should pick up and display the new user.

The 'Add user' button allows you to add a username in yourself. You must however know the exact Windows username on the home computer – it is better to let the username be picked up automatically.

Click the 'Edit' link next to the name. Note that you can delete the user here too.

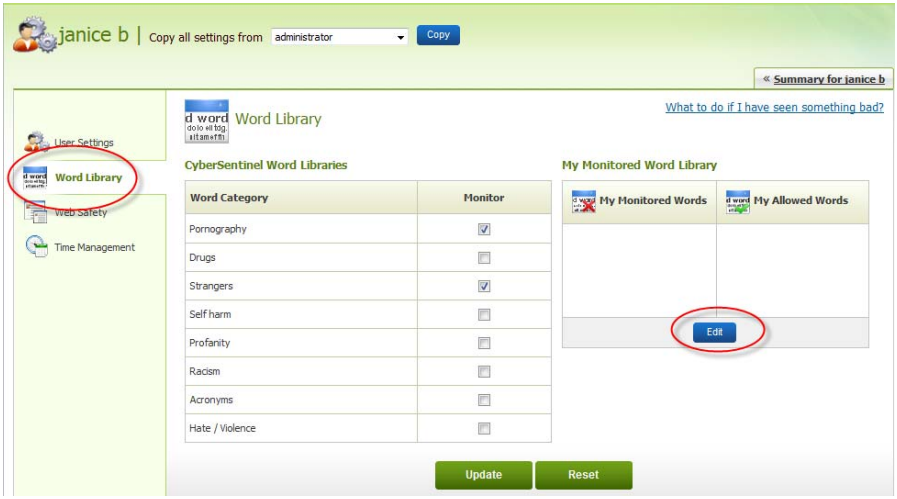
Step 4. Update the settings

The User Settings page will then be displayed, so choose the options as below to run the test.



Step 6. Display the Word Libraries

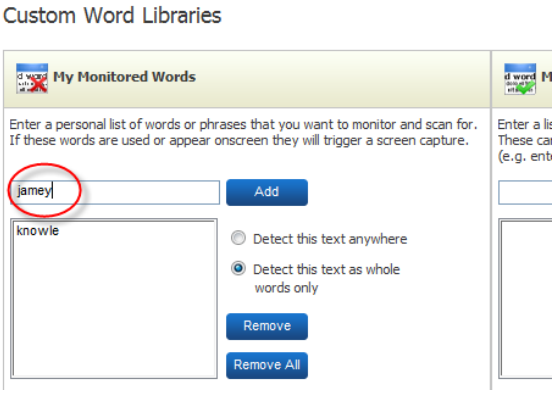
In the user settings window, choose the 'Word Library' tab.



Step 7. Monitor a special word

You will probably not want to have to type profanities for testing (we imagine!) so we advise that you use a word for testing that is unusual but otherwise inoffensive (e.g. princess – or dummy)

Add your test word to 'My Monitored Word Library' by clicking on the Edit button and then adding the word to the Blocked Words list. Use the 'OK' button to save the contents and exit the page.


Custom Word Libraries
My Monitored Words
Enter a personal list of words or phrases that you want to monitor and scan for.
If these words are used or appear onscreen they will trigger a screen capture.
jamey
Add
knowle
Detect this text anywhere
Detect this text as whole words only
Remove
Remove All

Running the word capture test

To test that the software is working correctly for generating screen captures, you need to use a computer with the CyberSentinel home software installed and logon as a user that has been configured in the Console.

You can have the console website open on the machine that you are testing to make the test easier to run.

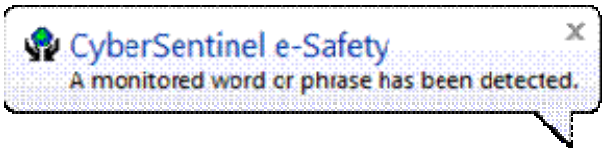
Step 1. **Logon at that computer with the user name that you are testing.**

Step 2. **The Acceptable Use Policy (AUP) should be displayed.**

Step 3. **Select 'Agree' to proceed and display the user environment.**

Step 4. **Create a violation by typing the test word into an application such as Notepad or Microsoft Word.**

Step 5. **The 'Violation' warning should be momentarily displayed in the bottom right of the screen.**



Return to CyberSentinel Console and go to the 'Home' screen.

Step 6. **In the recent captures list, you should see a small picture of the screen that you were just using.**

Step 7. **Double-click to check that you were correct.**

Step 8. **Go back and remove the dummy word if this is not a real 'bad' word.**

How to run the website test

To test that the software is working correctly for generating website logs, you need to use a computer with the CyberSentinel home software installed and logon as a user that has been configured in the Console.

You can have the console website open on the machine that you are testing to make the test easier to run.

Step 1. Login at the computer with the user name that you are testing

Step 2. Open a browser window

Step 3. Visit several web sites.

Return to CyberSentinel Console and go to the 'Home' screen.

Step 4. Select the user's link in the 'Home' screen.

Step 5. Select the 'Web Logs' tab to display the log of all the websites visited.

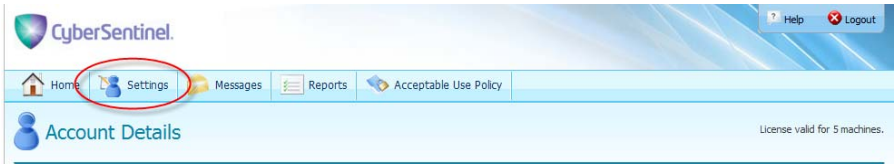
Step 6. The sites recently visited should be displayed.

Step 7. Repeat this test with different users to ensure correct functionality.

How to tell what machines are monitored by CyberSentinel

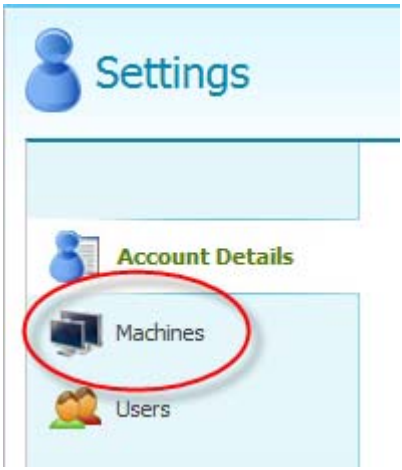
Step 1. Display the Account settings page

Click on the 'Settings' tab in the console



Step 2. Display the machines data

Choose the 'Machines' tab on the Left hand Side



You will see a list of computer names. Each computer is either 'Active' or 'Inactive'. This means that CyberSentinel is installed on those machines.

You can have up to 5 active machines per license.

A timestamp indicates the last time that the machine was communicating with the CyberSentinel Server.

Machines

Total : 5	Page 1 of 1		Go to page Go
PC Name	**Active**	**Inactive**	**Last Server Communication**
DELL-GGL	○	◉	13 Jan 09 13:20:20
DELL-GGL	○	◉	10 Feb 09 15:12:39
MUM-PC	◉	○	17 Feb 09 18:23:21
TESTPC	○	◉	11 Feb 09 10:44:36
USER-PC	○	◉	13 Jan 09 12:29:09
Total : 5	Page 1 of 1		Go to page Go

Update Reset

How to Add a User to CyberSentinel

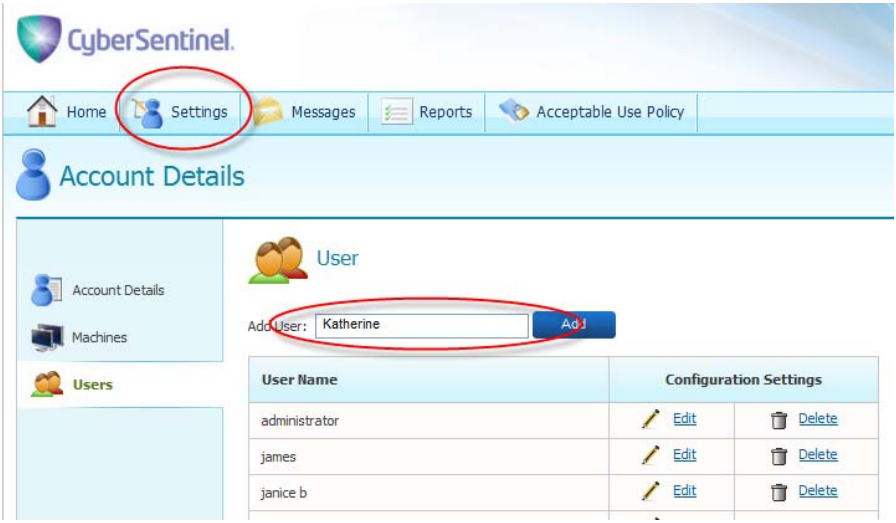
Each user account on a computer with CyberSentinel installed has a matching user file in your account on the CyberSentinel database.

If the user is not already known to CyberSentinel (because you have just installed the software, or just created a new user), a new file is created.

You can pre-create a new user account with the required settings before a user logs in to the computer after you have installed CyberSentinel – making sure that you only get the data that you want for each child.

Step 1. **Select 'Settings' tab**

Step 2. **Choose the Users tab**



Step 3. **Add the user name**

Step 4. **Select the 'Add' button**

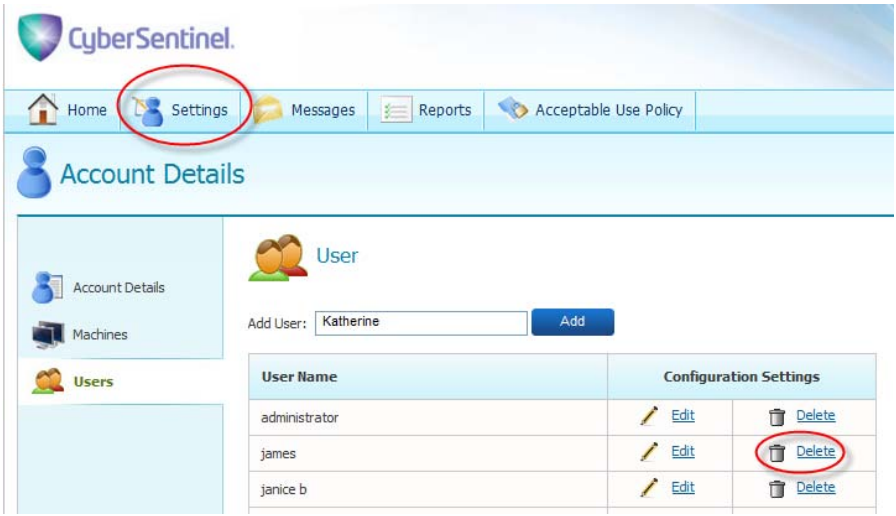
The name has been added to your account and is now displayed in the list of all users.

How to delete a user from CyberSentinel

If details of a user are no longer required, then the user account and all data associated with it can be deleted from the database by

Step 1. **Select 'Settings' tab**

Step 2. **Choose the Users tab**



Step 3. **Delete the user**

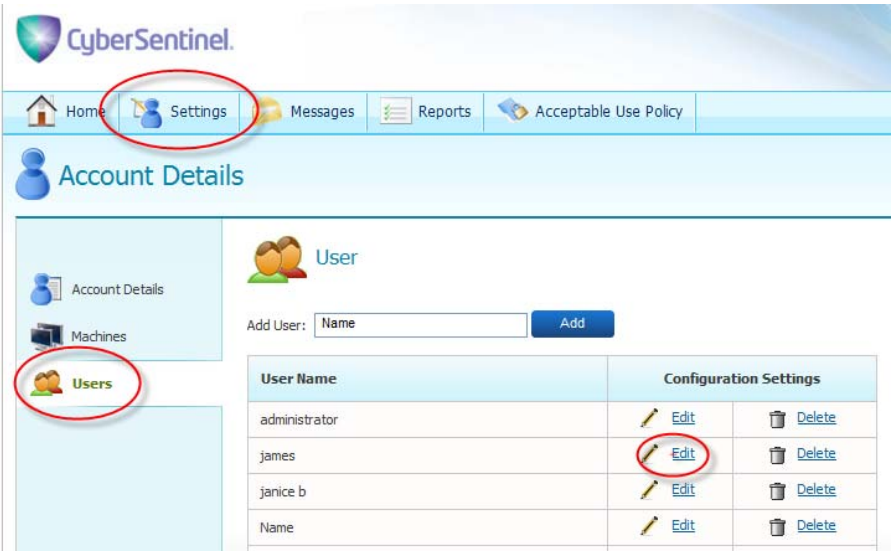
Select the 'Delete' link next to the user name that you would like to remove. Then confirm the delete from a popup window and the user is removed.

How to copying settings from one user to another

This feature allows you to copy the settings of one user to one or more of the other users that exist. This can be useful when configuring many users at once. Existing settings will be overridden.

Step 1. **go to the 'Settings' tab**

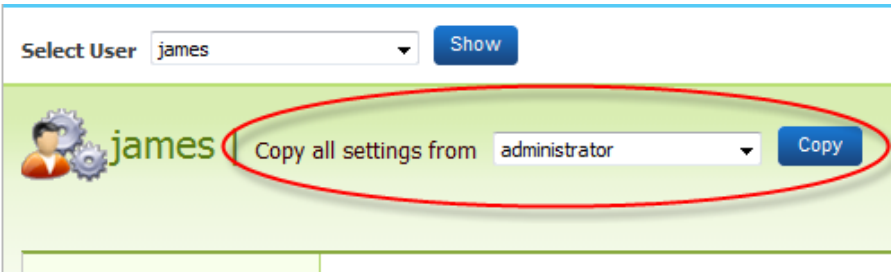
Step 2. **choose the 'Users' tab**



Step 3. **Edit the user's settings**

Select the 'Edit' button next to the user that you wish to assign the new settings to.

Step 4. **Copy**



Use the dropdown to choose the user that has the settings that you wish to copy. Then press the Copy button.

The users will now have the same settings. If you make changes to the first account, they will not be automatically copied, so you would have to copy them again.

Recommended User Settings

You can change the settings for your users so that they are suitable for their ages and interests.

This table shows all the settings with recommended values for normal use for a child and for a teenager.

You can change them depending on the circumstances of each child.

Item	Value	Explanation	child	teenager
Operation	Visible	The icon is visible on the screen and warnings are displayed		
	Invisible	Used if you do not want the user to know that they are being monitored		
	Suspended	Used if you want to stop CyberSentinel monitoring for this user		
Internet Chat is	On- unmonitored	The user is allowed to use Chat and it is not recorded		
	On – Monitored	The user can use chat, but the conversations are recorded so you can view them		
	Not allowed	The user is not allowed to use chat at all		

Check for blocked words every	10-150 seconds	This is the time between scans of the screen to check for bad words	10	60
Website logging is	On	Records the websites that are being visited by the user and the amount of time that is spent on them	On	Off
Word Library		Each of the word libraries has the option to block them for maximum scanning.	Block all	Don't block
Site libraries		Each of the site libraries has the option to filter	Block all	Don't block
Use scanning	Checked	This means that any website can be viewed so long as it is not in the libraries of blocked websites	No	Yes
Computer Quota Time	0-24 hours	With this option you can determine how long your child can access the computer per day. It will log them off at then of the quota time		

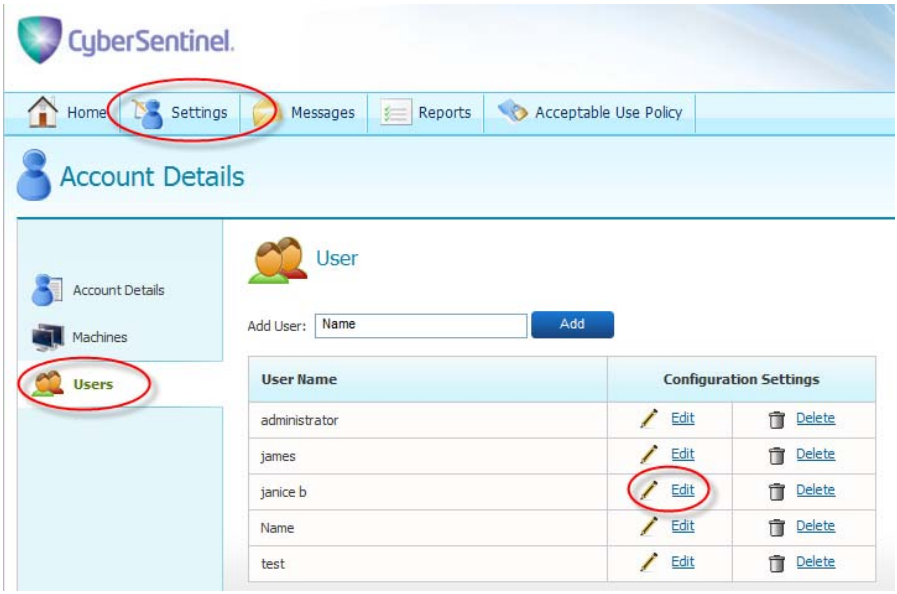
Configuring a user's Monitored Words

This tab is used to configure which libraries of words and phrases will be used when scanning the screen for undesirable words or phrases. It works on all non-picture applications.

The Word filter can analyse data that is being displayed and also data that is being typed on the keyboard.

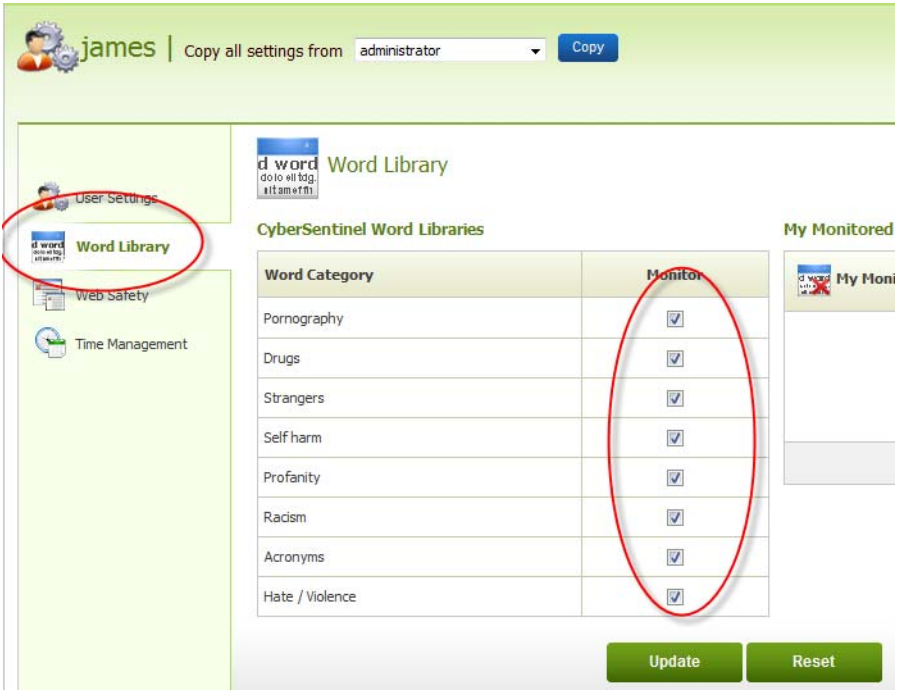
Step 1. Go to the 'Settings' tab

Choose the 'Users' tab



Step 2. Edit the user

Select the 'Edit' link for the required user and then choose the Word Library Tab in the User Settings screen.



Check the boxes beside the word libraries that you want to monitor for this user. For example, for very young children, you may want to check each box. But for older children you might just want to check the 'Self harm' box. Click here for a detailed description of the library contents.

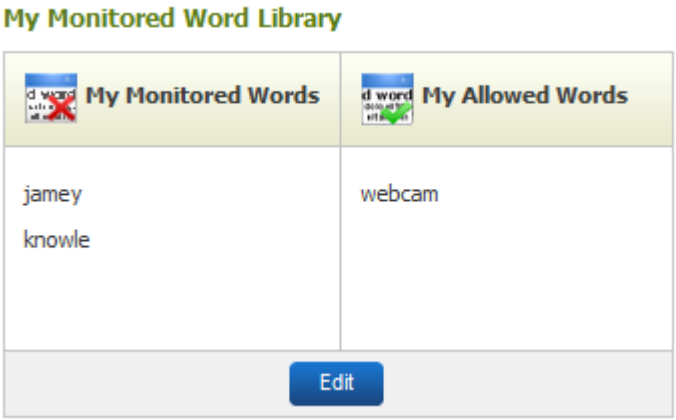
If you have any words that you want to specifically monitor, then edit 'My Word Library' by clicking on the 'Edit' button and then using the popup window to add or remove words from the lists. You might like to add the children's birthdays or mobile phone numbers in here so that you will be warned if they are distributing this information. Click here for more details about your customised library.

What is in the word libraries?

Library Name	Description
Pornography	This library covers areas such as Pornographic terms, sexual acts, sexual violence, sexual slang and profanity associated with sexual behaviour.
Strangers	This library covers areas such as Paedophilia, 'grooming' and child abuse. It contains phrases as well as individual words.
Profanity	This library contains common profane words and phrases, along with slang terms.
Acronyms	This library covers areas such as Chat Room use, colloquial and textual acronym slang. For Example:: ASL, FOAD
Drugs	This library covers the subject of drugs, including names, slang and usage.
Self harm	This library covers the subject of suicide, self-harm and depression.
Racism	This library covers common aspects of racism, including abusive terms and slang.
Hate/Violence	This library covers areas such as bullying, threatening behaviour, terrorism and use of weapons.

The ‘My Word’ Libraries

There are sure to be some words or phrases that you would like to monitor – or to exclude from monitoring. This can be done by editing your own library.



My Monitored Word list

This Library contains a list of words and phrases which will cause CyberSentinel to take a screen capture if detected. It should contain words and phrases specific to your family and this user. For example new slang words that you have noticed.

You might like to add the children’s birthdays or mobile phone numbers or even a string of number from your credit card in here so that you will be warned if they are distributing this information.

Be careful to avoid adding a term that is too general (such as ‘GAME’) which would create many ‘false-positive’ screen captures.

My Allowed Word Library

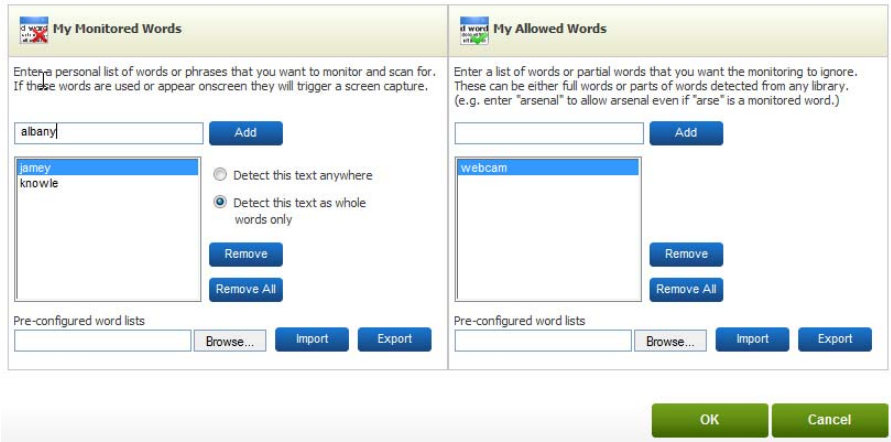
This Library is a list of words and phrases that you want CyberSentinel to ignore and therefore not cause a screen capture again for this user. If a word is contained in the CyberSentinel libraries as an embedded – or partial – word, then it is not possible to exclude words that contain that partial word.

This feature should be used with caution to avoid accidentally excluding a word that could indicate unacceptable use in some circumstances, especially if you are marking it as embedded.

How to Edit the Word lists

Add / Remove Words

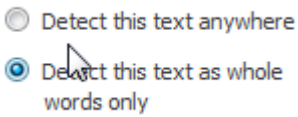
Enter the word or phrase in the field provided then click on the 'Add' button to submit it to the list.


My Monitored Words
Enter a personal list of words or phrases that you want to monitor and scan for. If these words are used or appear onscreen they will trigger a screen capture.
albany
Add
jamey
knowle
Detect this text anywhere
Detect this text as whole words only
Remove
Remove All
Pre-configured word lists
Browse...
Import
Export
My Allowed Words
Enter a list of words or partial words that you want the monitoring to ignore. These can be either full words or parts of words detected from any library. (e.g. enter "arsenal" to allow arsenal even if "arse" is a monitored word.)
Add
webcam
Remove
Remove All
Pre-configured word lists
Browse...
Import
Export
OK
Cancel

Use the 'OK' button to save the contents and return to the previous screen.

Specify Partial or Whole words in Monitored Word list

Each new word or phrase added to this library can be tagged as either 'detect text anywhere' (a partial word possibly embedded in another word) or 'Match whole words only' (a whole word). The default is whole word.



A ‘detect anywhere’ word or phrase will trigger a violation if it is contained within another word as well as if it occurs separately.

A word or phrase tagged as ‘whole only’ triggers a violation if discovered as a separate word.

The table below illustrates whether a violation would be triggered for the word ‘man’ in the following examples.

Example text	Whole word	Detect anywhere
The man walked down the road	Yes	Yes
www.demanding.com	No	Yes
My Grandma never forgets my birthday	No	No

Note that even for detect anywhere words, there can be no spaces in the word.

To indicate that the word is to be detected anywhere, select the word in the list and choose the top option.

Remove Words

Select a word on the list and press the remove button to take it off the list.

Use the ‘Remove All’ button to completely clear the list.

Get Word List

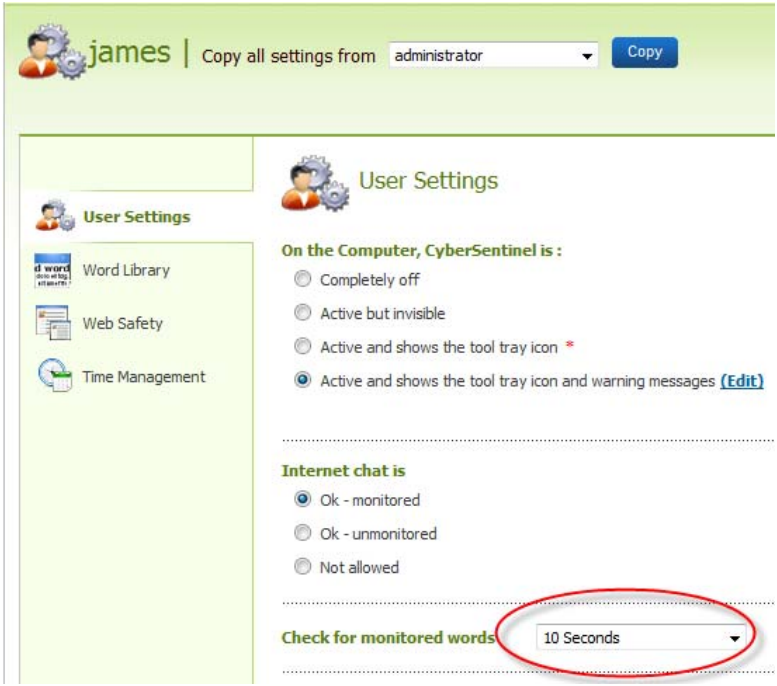
This feature allows you to import the current list of words from a text file. This is useful if you want to retrieve a list created by another user.

Save Word List

You can also save your own list of words to a file so that you could distribute it to another user.

How often should the word monitor work?

In the User settings page, you can control how often the screen is scanned for monitored words.



The trade-off for making this scan more frequent is that it takes a little bit of time, but if you make it too long, you might miss things – especially in a busy chat session or if the user is scanning lots of websites for pictures.

Different CyberSentinel modes

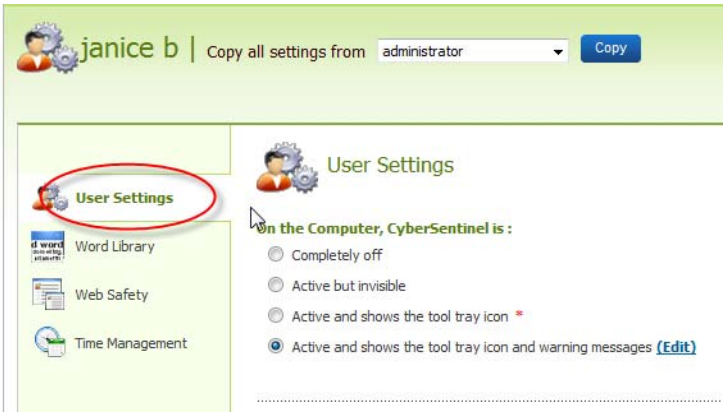
If **Active + ToolTray + Warning Messages** mode is selected for a user, the CyberSentinel icon will appear in the system tray as an indicator that the client software is present on the computer and a warning message will be displayed if a capture has been taken. It is not possible to close or otherwise stop CyberSentinel from working even if the icon is displayed unless you know the administrator login details.

If **Active + ToolTray** mode is selected for a user, the CyberSentinel icon will appear in the system tray as an indicator that the client software is present on the computer but no warning messages are displayed if a capture has been taken. This is a good way to remind a user that the software is present on their computer.

Active + Invisible mode means that CyberSentinel will not display its icon or any warning pages but the software is still functioning. The user need not be aware that they are being monitored.

Completely Off will mean that CyberSentinel is not running for that user at all; however the icon is displayed with a cross in it to indicate that is case.

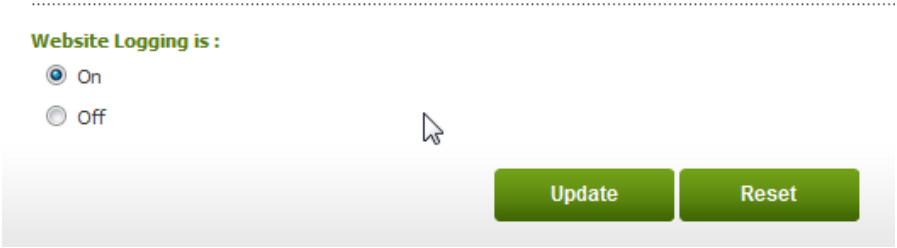
To change the mode, go to the User Settings page for the User whose configuration you wish to change then choose the option you require.



How to log Websites

CyberSentinel contains different features to control what website content is available

Selecting this option in the user account settings will allow CyberSentinel to seamlessly log all web site access for this user. This is independent of any filtering of websites.



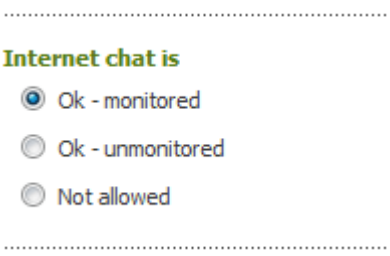
Logging of web sites will occur if the web page is displayed in most popular browsers such as Internet Explorer or Firefox or Chrome.

The data logged is

- computer
- user
- URL
- date
- time start and time finished

See the ‘Logs’ and ‘Reports’ section of this manual for the display that is generated.

How to Log Internet Chat

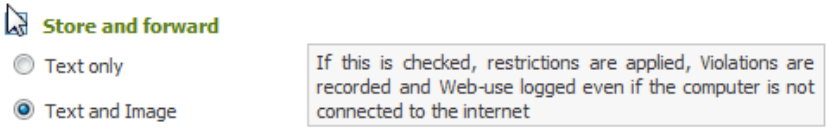


Selecting this option will let CyberSentinel record usage of some popular 'Instant Messaging' applications. An entire transcript of the conversation will be stored along with date, time and user information.

Chat logging will work for all ids that the child is using for each chat program.

You can view the chat logs in the Chat window, see here for details.

Offline Settings


Store and forward
Text only
Text and Image
If this is checked, restrictions are applied, Violations are recorded and Web-use logged even if the computer is not connected to the internet

These settings control how CyberSentinel client software should function when the computer is physically disconnected from the Internet.

Disable CyberSentinel Client

Un-ticking the 'Store and forward' option will disable all of the features of CyberSentinel if the computer is physically disconnected from the Internet.

Store and Forward

This feature allows the CyberSentinel Client to continue operating even though access to the Internet is not available. This is commonly used for computers that are periodically removed from the physical network, such as laptops.

If this option is selected, screen captures are stored locally and then uploaded to the CyberSentinel server computer when it is available.

Text Only

Selecting this option will permit the computer to store unlimited data of AUP acceptance/refusal, web sites, chat and violations but no screen captures will be stored.

Text and Graphics

Selecting this option will permit the computer to store unlimited data of AUP acceptance/refusal, web sites, chat and violations and up to 20 screen captures.

Configuring a User's Web Safety

CyberSentinel contains different features to control what website content is available to view on the computer. The available controls are listed below.

Specifically allow a selection of web sites - known as 'white listing' – these are sites that you know to be acceptable for your child

- Choose categories of acceptable websites.
- Specifically allow a selection of web sites - known as 'white listing' – these are sites that you know to be acceptable for your child and you do not want them to go to any others.
- Specifically block a selection of web sites – known as 'black listing' – these are sites that you do not want your child to access regardless of any other settings.
- Specifically block websites that contain certain words/phrases. This is useful where there are many different websites around a common theme and you want to block access to all of them. For example, websites about a particular Music group or computer game

Use the steps below to modify a user's web safety. An example of the configuration screen is shown overleaf.

Step 1. Go to the 'Settings' tab

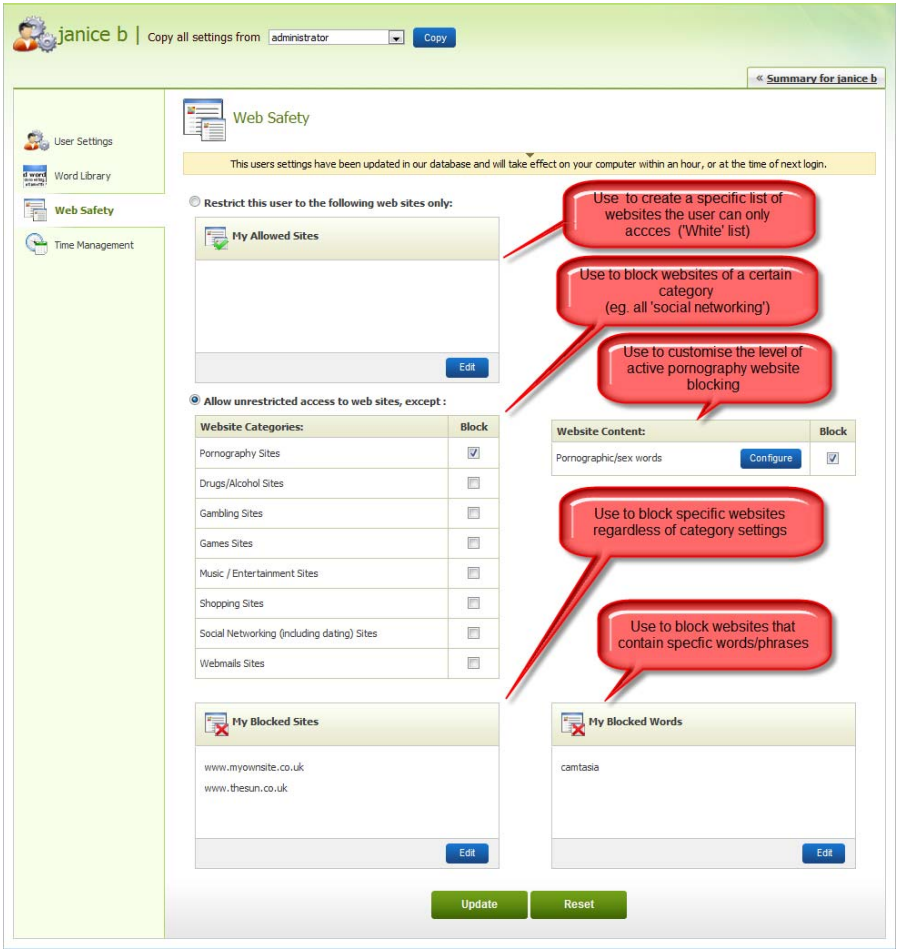
Choose the 'Users' tab

Step 2. Edit the user

Select the 'Edit' link for the required user and then choose the 'Web Safety' tab in the User Settings screen.

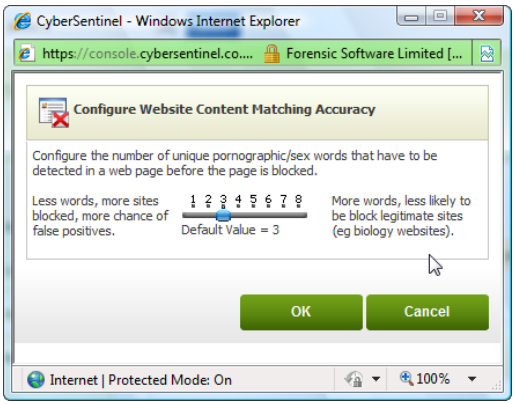
Modify the contents of the page to reflect how that users access to websites. For example, you may restrict a young user to your own specific (white) list of websites whereas an older user may just have certain categories of websites blocked.

More details and examples of these settings are in the next chapter of this manual.


janice b | Copy all settings from administrator Copy
« Summary for janice b
User Settings
Word Library
Web Safety
Time Management
Web Safety
This users settings have been updated in our database and will take effect on your computer within an hour, or at the time of next login.
Restrict this user to the following web sites only:
My Allowed Sites
Edit
Use to create a specific list of websites the user can only accces ('White' list)
Use to block websites of a certain category (eg. all 'social networking')
Use to customise the level of active pornography website blocking
Allow unrestricted access to web sites, except :
Website Categories:
Block
Pornography Sites
Drugs/Alcohol Sites
Gambling Sites
Games Sites
Music / Entertainment Sites
Shopping Sites
Social Networking (including dating) Sites
Webmails Sites
Website Content:
Block
Pornographic/sex words
Configure
Use to block specific websites regardless of category settings
Use to block websites that contain specfic words/phrases
My Blocked Sites
www.myownsite.co.uk
www.thesun.co.uk
Edit
My Blocked Words
camtasia
Edit
Update
Reset

CyberSentinel contains an advanced recognition engine to block access to pornographic websites based on the type of words/phrases often found in them in conjunction with a regularly updated list of this form of content.

Depending on your locale, you may find the engine blocks some legitimate websites due the words/phrases being found in them. If this is causing too many sites to be unnecessarily denied, you can modify the engine sensitivity by selecting the 'configure' button in the 'Website content' dialog.


CyberSentinel - Windows Internet Explorer
https://console.cybersentinel.co.... Forensic Software Limited [...
Configure Website Content Matching Accuracy
Configure the number of unique pornographic/sex words that have to be detected in a web page before the page is blocked.
Less words, more sites blocked, more chance of false positives.
1 2 3 4 5 6 7 8
Default Value = 3
More words, less likely to be block legitimate sites (eg biology websites).
OK
Cancel
Internet | Protected Mode: On
100%

Move the slider up and down and use 'OK' to confirm. This will have a direct effect on access to previously denied websites.

Website filtering by library categories

CyberSentinel includes a powerful Internet filtering service that we call ‘Categorised Scanning’.

If you use this facility for your children, it will monitor websites before they are displayed at the computer and reference against a selection of categorised libraries and your own customised black list.

If any word, phrase or URL is matched from these libraries then

- an optional warning dialog is shown to the child explaining why the page cannot be viewed.
- or a ‘redirect’ page will be shown to the user instead
- if web logging has been enabled for this user, then an entry will be made for this website that will be seen as red in the console log view

Website and word scanning differences

Web site scanning uses a similar library structure to Word Scanning but the two features are entirely different and can be used independently of each other.

Different categories of web content are used and can each can be 'blocked' by checking the box next to them. Attempts to view websites that fall into a blocked category will be denied.

The Word library categories are different because they are geared around the actual words/phrases found on websites or any other computer activity, such as Chat or within software applications such as games or word processors.

Website categories will stop the particular site being accessed whereas Word library will allow the activity to occur but take a screen capture of it taking place.

It is possible that a web page is judged by the website categories to be OK, but that the word scan will find an unacceptable word and a capture will be generated. In this way, you build up a much more useful overview of your user's computing activity.

Using Website Category Scanning

If you wish to allow a user to have access to websites other than those in a white list, then

Step 3. Go to the 'Settings' tab

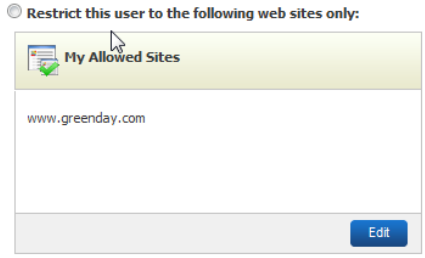
Step 4. Choose the 'Web Safety' tab

Step 5. Tick the relevant boxes to match the categories of websites to block.

You can block specific websites by entering their URL into the 'My Blocked Site' Library

My Allowed Site Library

The Allowed Site Library is a list of web sites which are NOT blocked or filtered, even though they may fall under one of the categories set to 'Block'. These sites can be viewed by the user regardless of their content although they may still generate violations from content viewed.



Add / Remove Sites from list

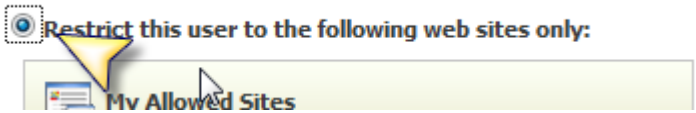
Enter the URL of a web site that the users are always allowed access to, even though it might be being blocked. For example, you may allow the user access to a single gambling web site for a project without enabling access to gambling web sites as a whole.

It is possible to enter specific URLs such as www.bbc.co.uk or use wildcards. For example, *bbc* would allow any URL with bbc in it and www.google.* would allow www.google.co.uk and www.google.com

Use the 'Remove' button to remove a highlighted entry from the list or the 'Remove All' button to clear the entire list.

Creating a 'White' list

If you want this list of websites to be the only websites that the user can access (a 'white' list) then tick the 'Restrict this user to the following web sites only' option.



Import/Export

The Export List button will copy the contents of the list to a text file for future use elsewhere.

The Import button can be used to import a text file containing entries to add to the list.

My Blocked Site Library

The Blocked Site Library is a list of web sites which are blocked, independent of the categorised scanning libraries. This can be useful to instantly stop new web sites that have just been discovered. It is managed in the same way as 'My Allowed Site Library'

It is also possible to add web sites to this list from the 'Logs' view and more details on this facility are explained in the 'Logs' chapter.

Time Management

CyberSentinel contains three features to control how the user spends their available time on the computer.

Internet Time Management

This feature is used to disable Internet access between certain half-hours of the day, on different days of the week. This covers all activities that require external Internet access, including online content, games and use of email programs.

Daily Computer Usage

The feature controls how much time the computer can be switched on and logged in during a 24 hour period. For example, you may wish to limit a user to three hours of computer time to be spent during a single day.

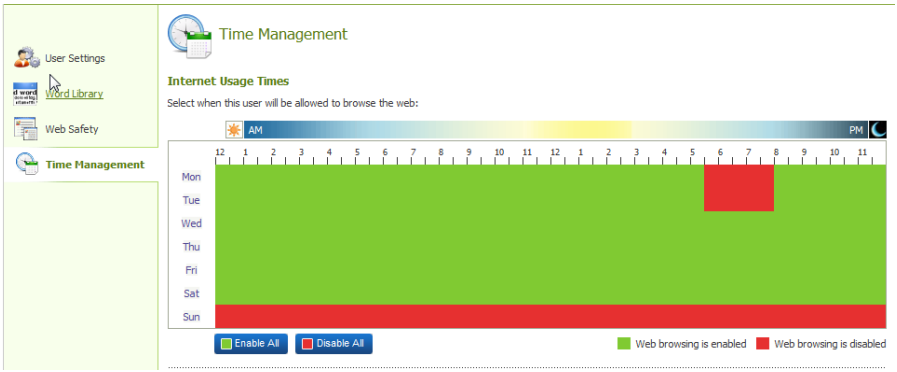
Application Usage

The feature can be used to limit the amount of time a specific application can be used during different days of a seven day period. For example, you may wish to limit use of a particular game to ‘Saturdays only’ or a maximum of one hour a day.

Configuring Internet Time Management

Step 6. **Go to the 'Settings' tab**

Step 7. **Choose the 'Time Management' tab**



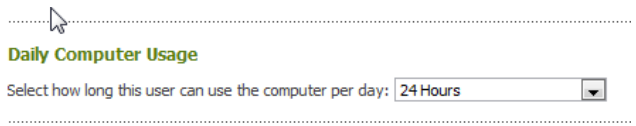
Select the time periods where Internet usage is to be controlled and use the 'Update' button to save these settings.

Individual days can be selected using the checkboxes provided and the Enable All/Disable All buttons will quickly change the entire contents of the window.

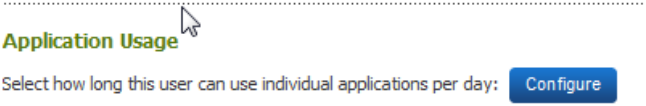
The advantage of using this feature in CyberSentinel rather than in the operating system or via a security program is that you can do it remotely and for all computers, rather than having to log onto each computer separately.

Configuring Daily Computer Usage

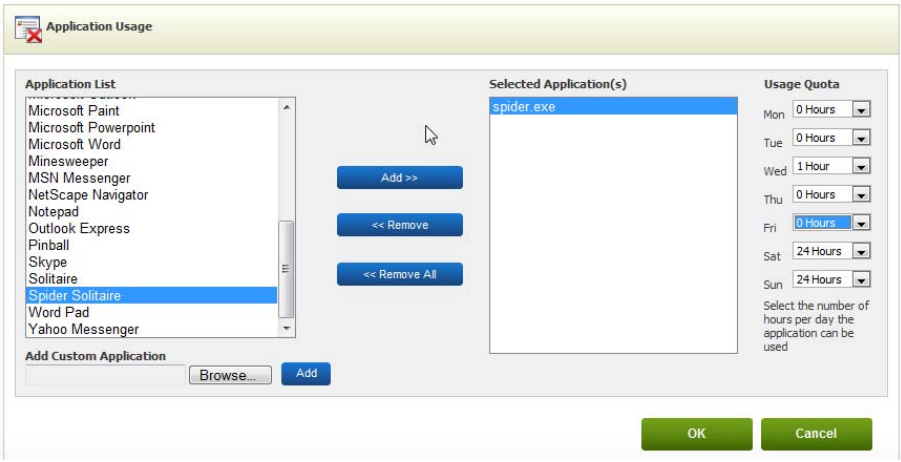
From the same dialog as above, select the amount of time for computer use in a 24 hour period using the pull-down menu. Use the 'Update' button to confirm this. Any attempt to use the computer outside this period will cause it to be shut down.



Configuring Application Usage



From the same dialog as above, select the ‘Configure’ button to display this dialog.



Select the application that you wish to control either in the listor by browsing to the local file on the computer using the ‘Browse’ button.

Use ‘Add’ to insert into the ‘Selected Application’ list and use the ‘Usage Quota’ pull-down menus to set the usage quota for each day of the week.

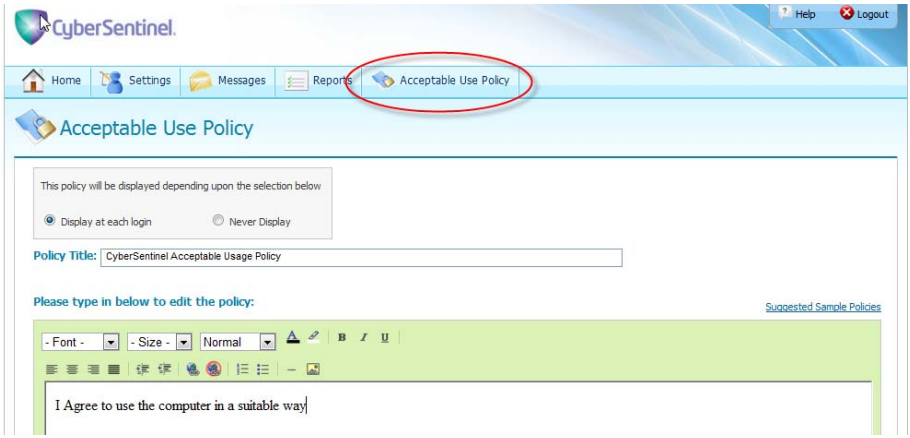
Once complete, use ‘OK’ to confirm and return to the previous dialog.

Setting up an Acceptable Use Policy

You should determine your own rules for your family and enter them in the language that is familiar to everyone. There is a link in the screen to a website with some suggestions for AUPs that other families have used.

When you have worked out the rules for your family, then follow these steps to write it up:

Step 1.Select the 'Acceptable Use Policy' button on the top menu.



Step 2. Type in the text that you expect everyone in your family to follow when using the computer

Step 3. Tick the box to say whether this should be displayed at each login.

Note: There is a limit of 5000 characters for the AUP text so that it fits on one screen.

Use the 'Update Policy' button at the bottom of the screen to confirm the new entry.

See here for a more formal description of an AUP

The Family Summary Data

This main display contains a summary of all the information in the CyberSentinel database recorded for everyone using your family computers. It is the first page displayed each time that you log in to the console.

1. The User list

The left hand column displays a list of all user accounts on the monitored computers. Next to them is the number of captures that are stored for that user, if there are unviewed captures, then the number is red, otherwise green.

2. The 'Most Viewed Websites' list

This shows the top 10 websites that are visited by your family. This gives you a quick snapshot of what kind of activity is taking place.

3. Recent Captures

These are the last 6 captures received from your computers. You can double click on any of them to see a bigger version (watch out for unsavoury images; check that no one is watching the screen who will be shocked). You can delete them straight away if they are of no concern.

4. Recent Messages

These are a few messages that you may be interested in regarding your account, including details of you license and any product maintenance that may be occurring.

The User Summary Data

Step 1. Choose the User

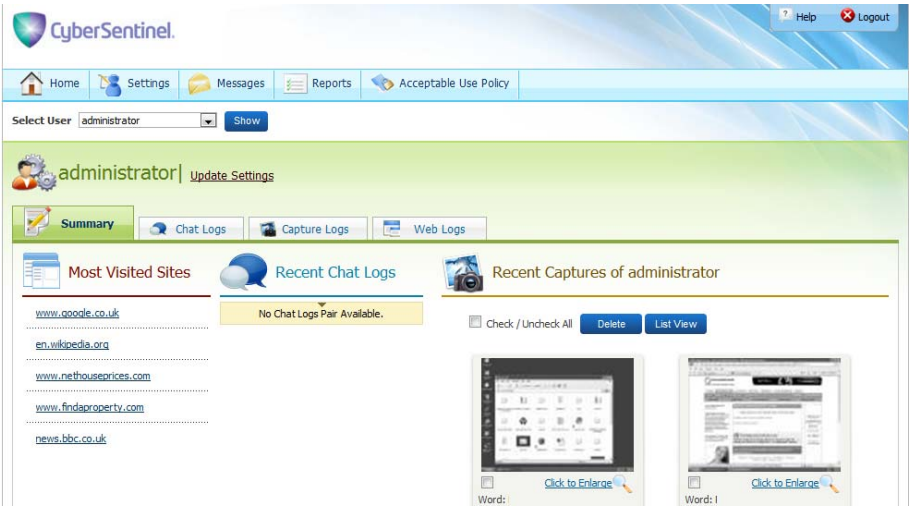
The User names in the Family Summary page are links to summary pages for each user that has an account on your computers. Click on the link to select the user you wish to view.

You will be navigated to a file for that user's data. The landing page is a summary for that user.

Step 2. Look at the summary

Often, all the information that you need is contained in the summary page for the user. You can easily see what websites are being visited and the captures.

If you wish to change the users settings, you can easily use the 'Update Settings' link next to the users name.



Step 3. Select the relevant tab

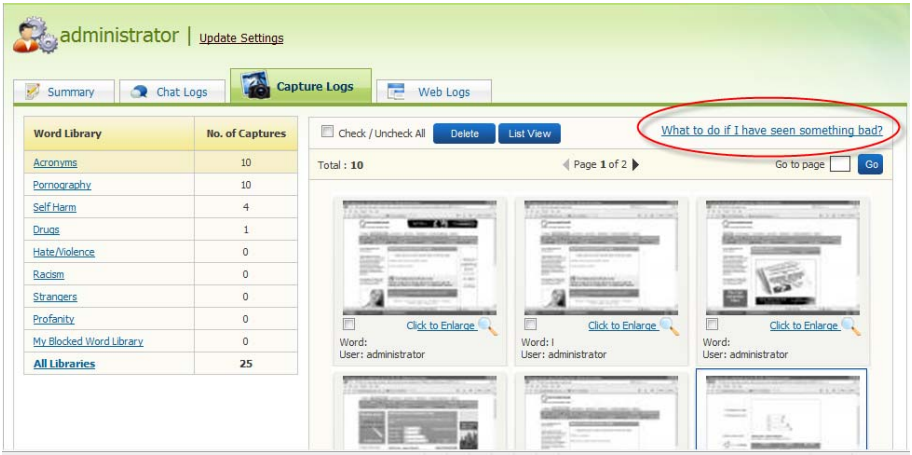
If you want to see more information, then use the file tabs to open a more detailed log of data:

Captures	Real-time screen captures indicating possible improper use, grouped according to category
Chat	Text recording of any chat conversations using MSN or other chat clients between any chat ids that are used while that user is logged in.
Web	Logs of all the web sites visited by the user showing the time spent

Viewing Capture Data

Remember that captures can be unpleasant to view.

If you see a capture that really worries you and you do not know what to do about it, click on the link 'What to do if you see something bad' for help.



The Captures that have been taken while the selected user is logged in to the computer are stored against the library that triggered them. For example, a capture generated because a swear word was detected would be viewed by selecting the 'Profanity' library.

You can see all the captures against a particular library by clicking on the library name. Note that the library you create is called 'My Blocked Word Library'. If there are no captures at all, then a message will be displayed indicating this.

You can double click on the thumb nail picture to bring up a full screen image and the details of the capture, i.e data, time, application and word that generated the capture.

Remember that, even if you are not monitoring Chat sessions or logging website usage, screen captures will still be taken wherever monitored words are encountered.

Viewing Chat Data

Selecting this tab will display transcripts of any chat conversations undertaken within MSN Messenger and other popular chat clients.

You can choose the particular conversation to view from the drop down list of conversations, then choose a day.

It is not possible to ever know when a conversation ends so they are all stored over a 24 hour day. The full transcript of the conversation will be shown, including the text from the other participants.

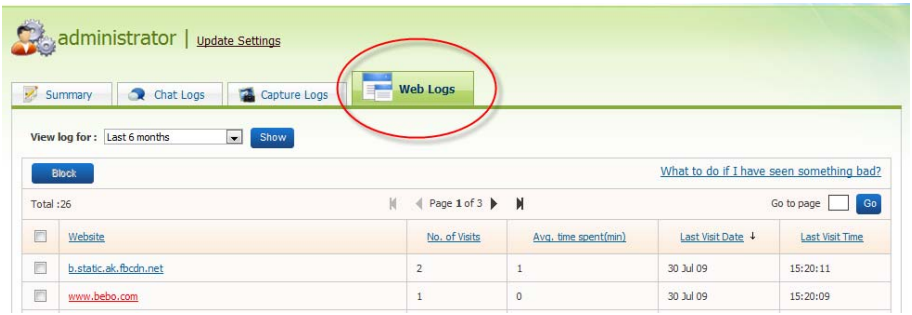
Note that it is often not easy to detect who a person is from the chat_id and your own child may well use different identities for chatting with different people.

Also note that if CyberSentinel detects a monitored word during a chat session, a screen capture will be taken and you can see it in the Capture Logs screen.

Viewing Web Log Data

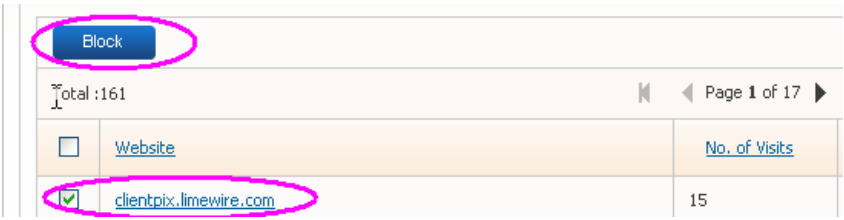
Selecting this tab will display all web sites accessed by the user, displayed in order of frequency of use, you can choose the time period to be considered for this display.

Please note that the time period 'Last 24 hours' means all sites visited since midnight last night.



There is only one record for each website so the data displayed is a summary of all visits to that site including: Number of visits, average time spent; the last access date and time.

You can view the website (in a new window) by clicking on the name which is a link to the site. The web site can be immediately blocked by selecting the box next to the name and then using the 'Block' button at the top of the list. This will add that URL to the 'My Blocked' list for this user.



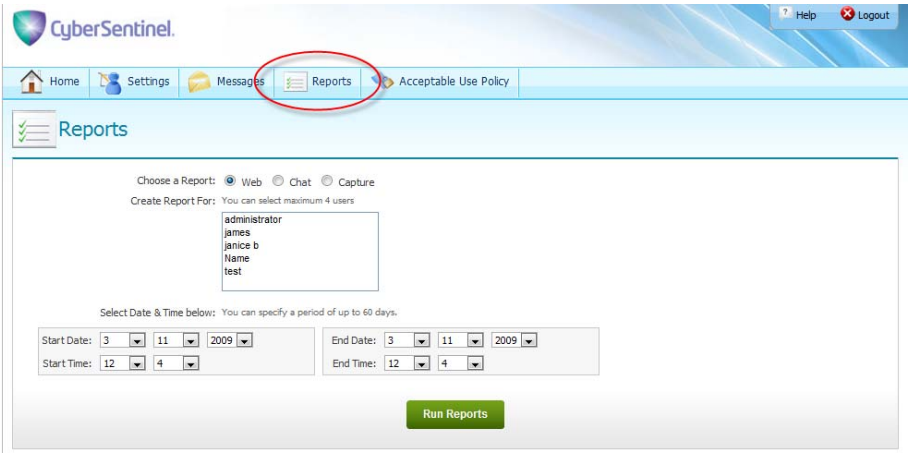
You can click on the headers of the list to re-order the log. For example if you want to see all sites visited on a particular day, click on the header .

If this user has attempted to access any of the blocked sites they will be recorded in red so that you will know about it.

Reports

The Reports tab allows you to generate some standard reports. These reports are produced using a limited selection of criteria. Once created, the reports can be exported in different industry-standard formats.

Step 1. Select the Reports tab to view the report categories.



Choose the type of report (web/chat/capture).

Choose up to 4 users whose data will be included in the report.

All reports can be set to show data from a certain date range using the 'date range' and 'time range' options up to a maximum of 60 days.

Step 8. Use the 'Run Reports' Button to generate the report.

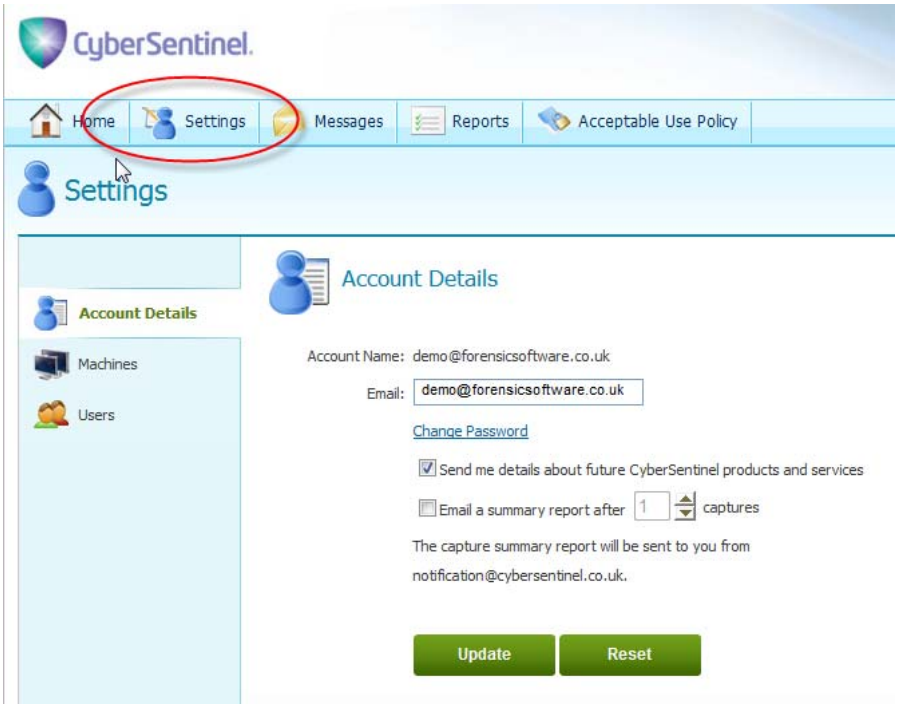
The report can be immediately viewed in a separate window and printed from the browser if required.

Step 9. Export the data to save it.

The data will be saved in .csv format which can be opened in many programs. If you have linked .csv files to open in a particular program, like Excel, then it will automatically open.

What are my account details?

There are some settings that apply to your account separately from the User Settings. They are accessed from the Account Settings tab in the top menu.



We know that occasionally you may like to change your email address for receiving reports and other notifications from us, so you can do it from this screen. Just type it in the email box and then click the green Update button.

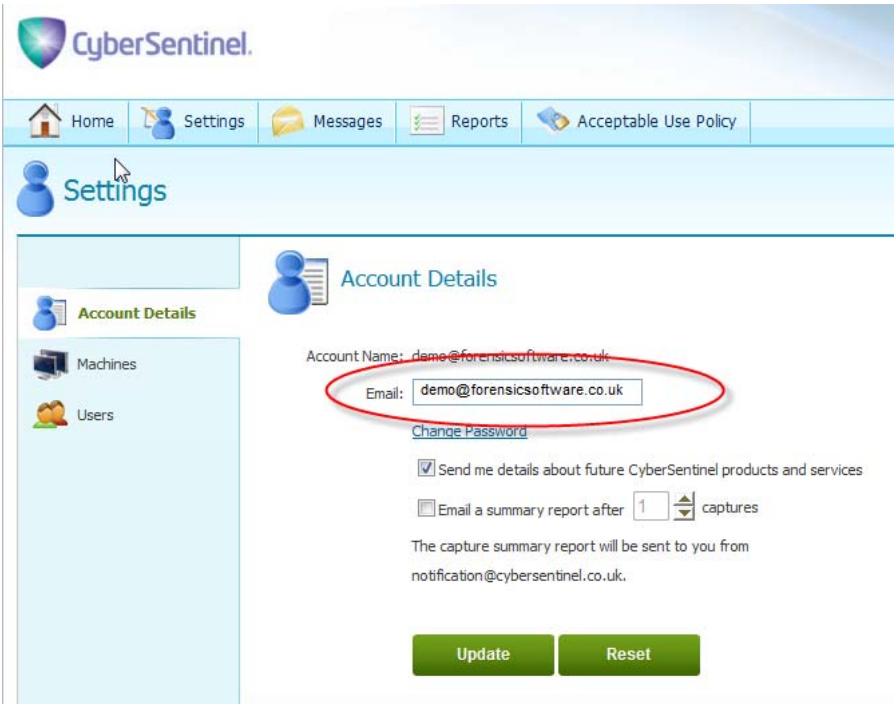
If you would like to be informed via email after a number of captures have been received, then you can set this here too.

You can turn off the receipt of marketing information by un-checking the box.

How do I change my email address?

When you register your account with CyberSentinel, you use an email address to create a unique identifier. This saves a lot of problems in establishing the account – but it means that if you change your email address it is no longer in step.

We cannot change your Account ID, but we do allow you to change the email address that is used to send summary reports and occasional other emails.

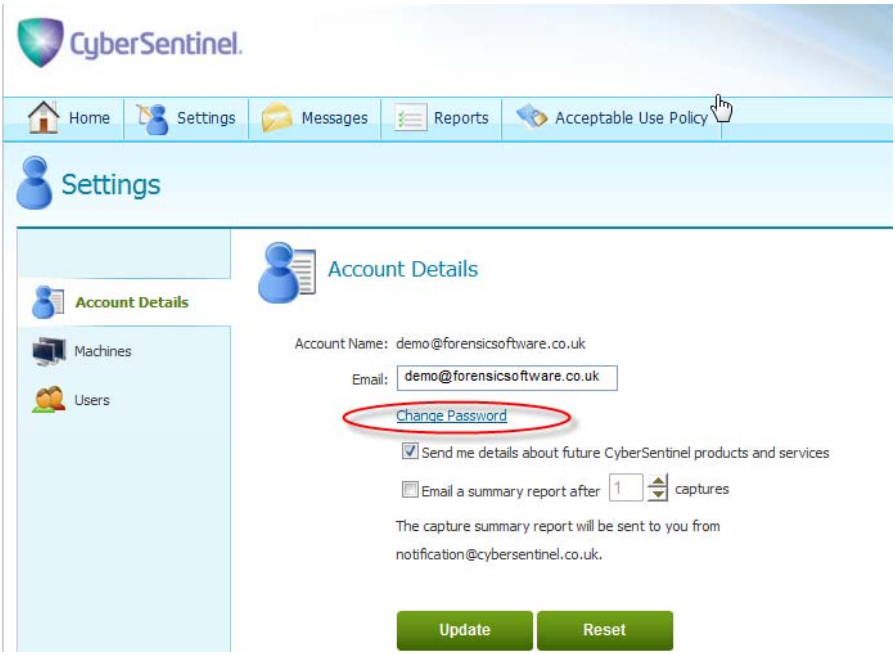


Enter the new email address in the field provided and use the 'Update' button to confirm. The new address will take effect immediately.

Remember this new address is will required to sign back into the CyberSentinel Console when you visit again.

How do I change my password?

You can change your account password in the Account Settings page

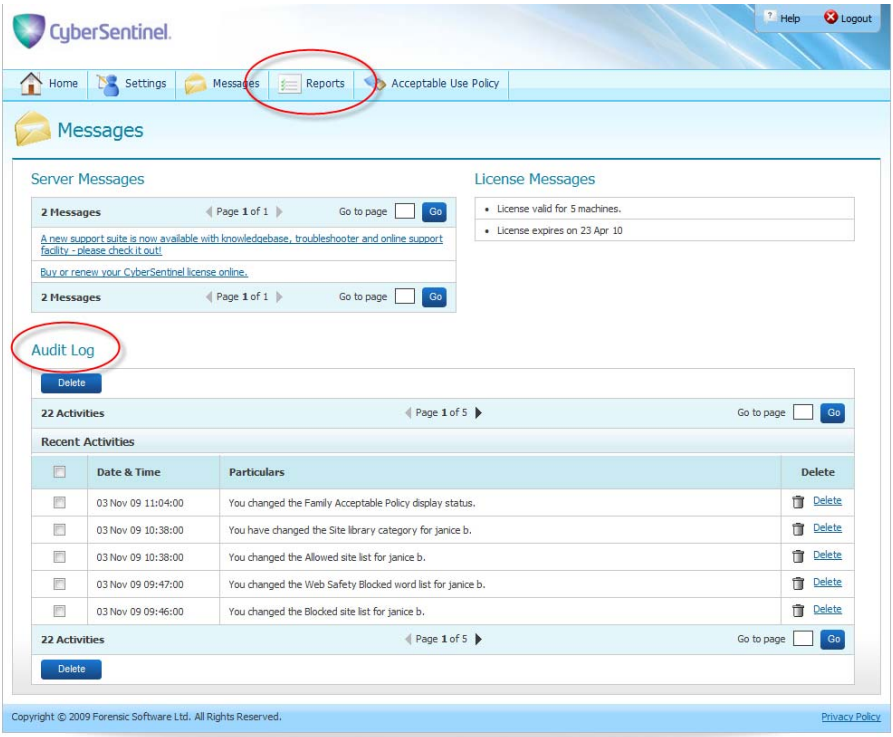


Another dialog box appears when you click on' Change Password'. Enter the required details here and use 'Save' to confirm.

Audit Messages

Every time you perform an administration task on the CyberSentinel Console, an entry is made to an audit log.

These are viewable in the Messages tab.



The kinds of things that generate an audit log entry are

- Updating the settings
- Copying the settings
- Adding or deleting a user
- Changing the libraries that are being blocked
- Adding words to any of the ‘my words’ libraries

What is an Acceptable Use Policy?

An Acceptable Use Policy is broadly defined as:

"A set of rules and guidelines that specify in detail the appropriate use of systems or networks. "

It reminds the user to make good choices about the use of the computer every time they log on.

Some of the most common resources that you might like to address in the AUP for your family are listed below.

- Internet usage
- Email usage
- Physical usage of computer hardware
- Use of the printer
- Data storage limitations
- Creation and/or distribution of inappropriate material
- Data protection and privacy obligations
- Software licence adherence

The parent will 'draw up' an AUP outlining the correct procedures and usage that all home users with which all users should comply. The users should all be made aware of, and agree to, the terms of an AUP before allowed to logon to the computer. The children should probably help to create it.

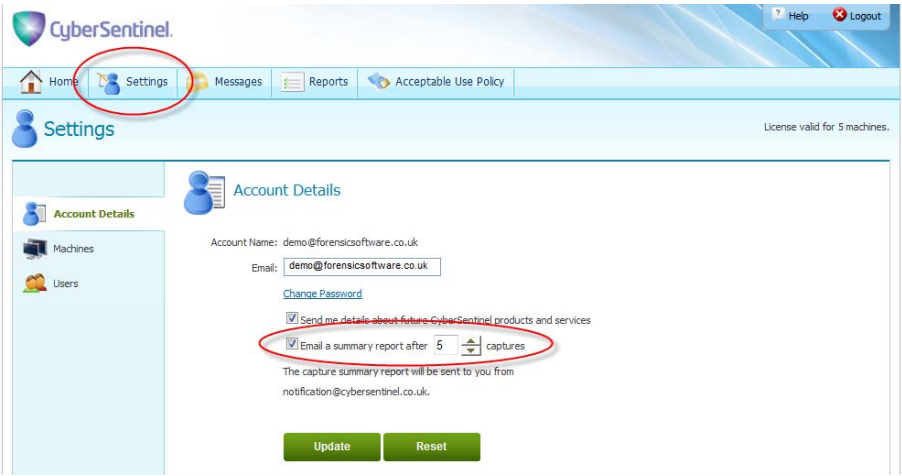
Doing this automatically means that you do not have to keep reminding children about your expectations – less nagging!

Can I receive emails from CyberSentinel?

CyberSentinel can send an email to the registered email address for your account when a certain level of new captures occur.

This feature is switched off by default. Follow the steps below to enable it.

Step 1. Select the 'Settings' button to display this page

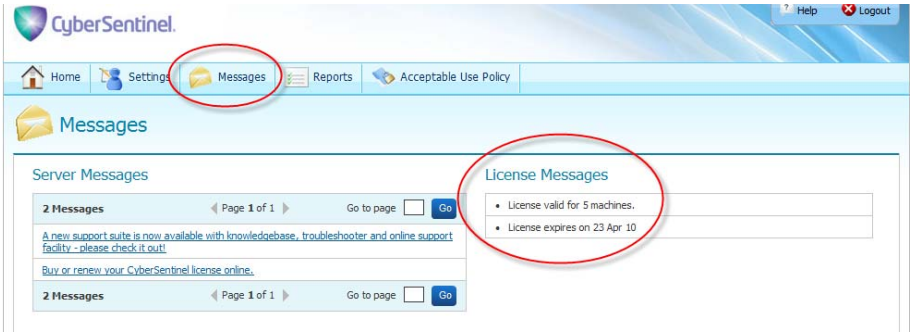


Step 2. Tick the box next to 'Email a summary report…' and enter a suitable value.

Use the 'Update' button to confirm. If you find that you are getting too many or too few emails then adjust the value accordingly.

How long is my license is valid for?

You can see how long your license is valid for in the 'Messages' tab. It also tells you how many machines you can install CyberSentinel on.



Glossary

Acceptable Use Policy / AUP	A set of rules and guidelines that specify the expectations of the user in regard to appropriate use of systems or networks. The growth of Internet use in the workplace and Education establishments has made an AUP virtually essential to ensure users utilise this resource in an acceptable manner.
Allowed Site Library	The allowed site library contains a list of web sites that are not subject to the categorised scanning restrictions and so can be viewed by the user.
Applications	Applications are the software and utilities installed on your computer. Microsoft Word is an application, as is Internet Explorer.
Blocked Site Library	The blocked site library contains a list of web sites that users are not permitted to view, regardless of their status within categorised scanning.
Blocked Word Library	The blocked word library contains a list of words and phrases that are not contained in the standard libraries, but will cause a violation. Typically, this contains words and phrases specific to your family.
(Screen) Capture	A capture is a graphic image of the computer use at the time that a word/phrase from the content of the built-in libraries or your custom library was detected.
Categorised Scanning	A function of CyberSentinel that allows web content of specific types, such as gambling or web mail to be blocked or allowed as desired. Attempts to view a blocked form of content are met with a warning dialog and the page is re-directed.
Chat	A feature offered by many online services that allows participants to 'chat' by typing messages which are displayed almost instantly on the screens of other participants who are using the chat room.

Chat Room	A website where people can chat with other people in the room. Chat Rooms are usually organised by a theme. A user can view all of the conversations taking place at once on their screen or have 'private chat' to just one person.
Console User	A user account that has access to CyberSentinel Console with permissions to view and/or modify user settings and view the data.
CyberSentinel Console	The web-based interface of CyberSentinel where all administration and reporting takes place.
Embedded	Embedded words/phrases are part of a whole word/phrase or the actual word/phrase itself. For instance, if the word MAN is embedded, then the words HUMAN and MANHOOD would trigger a violation because MAN is contained inside HUMAN and MANHOOD.
False Positive	The captures that are generated that turn out to be false alarms.
Instant Messaging	A web-based service that enables users to see whether another individual is currently online and to send that user a short message immediately, without the store-and-forward delays inherent in email. MSN Messenger is a popular Instant Messaging program.
Invisible Mode	If invisible Mode is selected for a particular user then the CyberSentinel icon is not visible in the system tray during normal use.
Non-Embedded	Non-Embedded words/phrases are whole words/phrases, and not parts of them. If the word MAN is non-embedded, then the words HUMAN and MANHOOD would not trigger a violation. Only use of the word MAN by itself would trigger a violation/capture.
URL	The standard way to give the address of any resource on the Internet that is part of the World Wide Web. A typical URL looks like http://www.amazon.com
Visible Mode	If Visible Mode is selected for a user then the CyberSentinel icon is visible in the system tray during normal use.

Further Help and Support

All technical support is provided via email. Please send all details to

support@cybersentinel.co.uk

And we will get back to you very soon.

Index

Acceptable Usage Policy
definition, 69
setting, *58*
Account Details, 40
Account id
can I change it, 41
Allowed site list, *53*
Blocked Site list, *54*
Capture logs
viewing the logs, 63
Chat logging
how, 45
viewing the logs, 64
Configure user account, 20
Console
login, 17
CyberSentinel
description, 6
CyberSentinel icon
what does it mean?, 43
Download to another computer, 16
Emails
can I change my address, 41
send a capture email, 40
summary report, 70
Embedded words, 37
Family data logs
Summary, *59*
Glossary, *72*
Hardware requirements, 13
Installation
hardware requirements, *13*
Home computer, *12*
Process, *14*
Software requirements, *13*
Testing, *19*
what machines are using, 25
Invisible mode, 43
license validity, 71
Messages
Audit logs, 68
Monitored words, 39
Offline settings, 46
Password
changing, 42
Remove CyberSentinel, 18
Reports
configuring reports, *66*
further processing, *67*
Software requirements
Operating system, 13
Store and forward, 46
Suspended Mode, 43
Testing
capture reports, 23
web logging, 24
text only captures, 46
Unembedded words, 37
User data logs
capture logs, *63*
chat logs, *64*
summary, *61*
web logs, *65*
Users
Add a user, 27
configure settings, 29
Delete a user, 28
recommended settings, 31
Visible mode, 43
Warning dialog, 50
Web logging
data recorded, 44
how, 44
testing, 24
viewing the log, 65
Website categories
compared to word libraries, *51*
configuring, *47*
definition, *50*
setting, *52*
Why use, 10

Website scanning
description, 8
Word libraries
compared to website categories, *51*
configuring, 33
description, 36
what is in them, 35
Why use, 10
Word lists, 37
Word scanning, 7
set the interval, 39

© Forensic Software Ltd 2009

All trademarks are acknowledged as the property of their respective owners.

No part of this document may be published, scanned or displayed in any other form without prior permission from the copyright owners.

Version 3.1.5.0

November 2009